Amendments To Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A method for registering and using a proffered biometric sample for facilitating a Radio Frequency (RF) transaction, ~~biometric information for use in a transponder reader system~~, said method comprising:

detecting ~~a~~ said proffered biometric sample at a biometric sensor ~~to obtain a proffered biometric sample~~;

associating said proffered biometric sample with at least one of an RF device, a user identifier, and a transaction account;

verifying said proffered biometric sample in order to activate said RF device and confirm said proffered biometric sample; ~~and~~

storing said proffered biometric sample as a registered biometric sample; ~~sample on a database such that said system utilizes said proffered biometric sample to authorize a transponder transaction.~~

receiving a transaction request from said RF device, wherein said transaction request comprises a transaction biometric sample; and,

authorizing said transaction request when said transaction biometric sample matches said registered biometric sample.

2. (Canceled)

3. (Canceled)

4. (Currently amended) The method of claim 1, wherein said ~~step of~~ detecting of said proffered biometric sample includes at least one of detecting, associating, and processing at least one additional proffered biometric sample.

5. (Canceled)

6. (Currently amended) The method of claim 1, wherein said ~~step of~~ verifying of said proffered biometric sample comprises ~~includes~~ comparing said [[a]] proffered biometric sample with a stored biometric sample.

7. (Currently Amended) The method of claim 6, wherein said comparing of said [[a]] proffered biometric sample with said [[a]] stored biometric sample includes comparing said [[a]] proffered biometric sample with at least one of an authorized and unauthorized ~~a~~ biometric sample ~~of a criminal, a terrorist, and a transponder user~~.

8. (Canceled).

9. (Currently amended) The method of claim 1, wherein said ~~step of~~ verifying of said proffered biometric sample includes verifying said [[a]] proffered biometric sample using at least one of a protocol/sequence controller and a third-party security vendor.

10. (Canceled).

11. (Currently amended) The method of claim 1, wherein said ~~step of~~ storing of said [[a]] proffered biometric sample includes storing said [[a]] proffered biometric sample on at least one of a local database, a remote database, and a third-party controlled database.

12. (New) The method of claim 1, wherein said verifying of said proffered biometric sample comprises comparing said proffered biometric sample with a verification biometric sample received from said RF device.

13. (New) The method of claim 1, wherein said biometric sensor comprises at least one of: a retinal scan sensor, an iris scan sensor, a fingerprint sensor, a hand print sensor, a hand geometry sensor, a voice print sensor, a vascular sensor, a facial sensor, an ear sensor, a signature sensor, a keystroke sensor, an olfactory sensor, an auditory emissions sensor, and a DNA sensor.

14. (New) The method of claim 1, wherein said proffered biometric sample comprises a biometric sample characteristic comprising at least one of: blood flow, correctly aligned ridges,

pressure, motion, body heat, ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore location, loops, whorls, and arches.

15. (New) The method of claim 1, wherein said user identifier comprises at least one of: personal information, financial information, loyalty point information, employee information, employer information, medical information, and/or family information.

16. (New) The method of claim 1, further comprising associating a second biometric sample with at least one of a second RF device, a user identifier, and a transaction account.

17. (New) The method of claim 1, wherein said biometric sensor is associated with at least one of: a local database, a remote database, a portable storage device, a host system, an issuer system, a merchant system, a fob issuer system, an employer, a financial institution, a non-financial institution, a loyalty point provider, a company, the military, the government, a school, a travel entity, a transportation authority, and a security company.

18. (New) The method of claim 1, further comprising:

transmitting a device authentication code from a sample receiver to said RF device;

receiving an encrypted device authentication code, a second proffered biometric sample, and a unique device identification code from said RF device;

decrypting said encrypted device authentication code using a unique device decryption key corresponding to said unique device authentication code;

comparing said decrypted device authentication code to said device authentication code; and

authenticating said RF device when said second proffered biometric sample matches said registered biometric sample and when said decrypted device authentication code matches said device authentication code.

19. (New) The method of claim 18, further comprising:

receiving an encrypted device account code from said RF device;

decrypting said encrypted device account code using said unique device decryption key; and

transmitting said decrypted device account code for processing.

20. (New) The method of claim 19, further comprising:

receiving a reader authentication code from said RF device;

encrypting said reader authentication code using a reader encryption key to create an encrypted reader authentication code; and

transmitting said encrypted reader authentication code to said RF device for authentication of said sample receiver.

21. (New) An authorized sample receiver (ASR) configured to register a biometric sample and facilitate a Radio Frequency (RF) transaction, said ASR comprising:

a biometric sensor configured to receive a first proffered biometric sample;

a communications device configured to receive a second proffered biometric sample associated with an RF device, wherein said ASR is configured to verify said second proffered biometric sample in order to activate said RF device, and wherein said ASR is configured to store said first proffered biometric sample as a registered biometric sample when said second proffered biometric sample matches said first proffered biometric sample;

an RF Identification (RFID) reader configured to receive a transaction request from said RF device, wherein said transaction request comprises a transaction biometric sample, an encrypted device account code, and a unique device identification code;

a plurality of device-specific decryption keys; and

an authentication circuit configured to select a unique device decryption key from said plurality of device-specific decryption keys by associating said unique device identification code with said unique device decryption key, and wherein said authentication circuit is further configured to use said unique device decryption key to decrypt said encrypted device account code; and

wherein said authentication circuit is further configured to compare said transaction biometric sample to said registered biometric sample in order to authenticate said RF device and facilitate said RF transaction.

22. (New) The ASR of claim 21, further comprising a USB interface configured to communicate with said RF device.

23. (New) The ASR of claim 22, wherein said USB interface is further configured to personalize said RF device.

24. (New) The ASR of claim 21, wherein said decrypted device account code comprises a device account number in a magnetic stripe format configured to be transmitted to a Point of Sale (POS) device and processed under a merchant's business as usual standard.

25. (New) The ASR of claim 21, further comprising an RFID reader PIN interface configured to receive a secondary verification.

26. (New) The ASR of claim 21, further configured to transmit a device authentication code to said RF device, receive an encrypted device authentication code from said RF device, and decrypt said encrypted device authentication code using said unique device decryption key in order to authenticate said RF device.

27. (New) The ASR of claim 21, further configured to receive an ASR authentication code from said RF device, encrypt said ASR authentication code, and transmit said encrypted ASR authentication code to said RF device in order to facilitate authentication of said ASR.